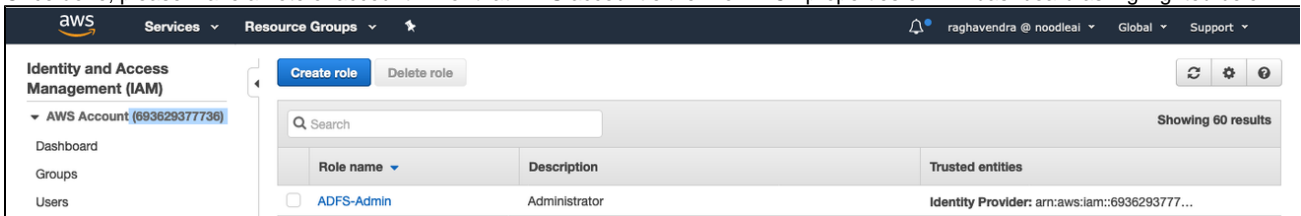


External Document - Adding more AWS accounts to Azure AD SAML authentication

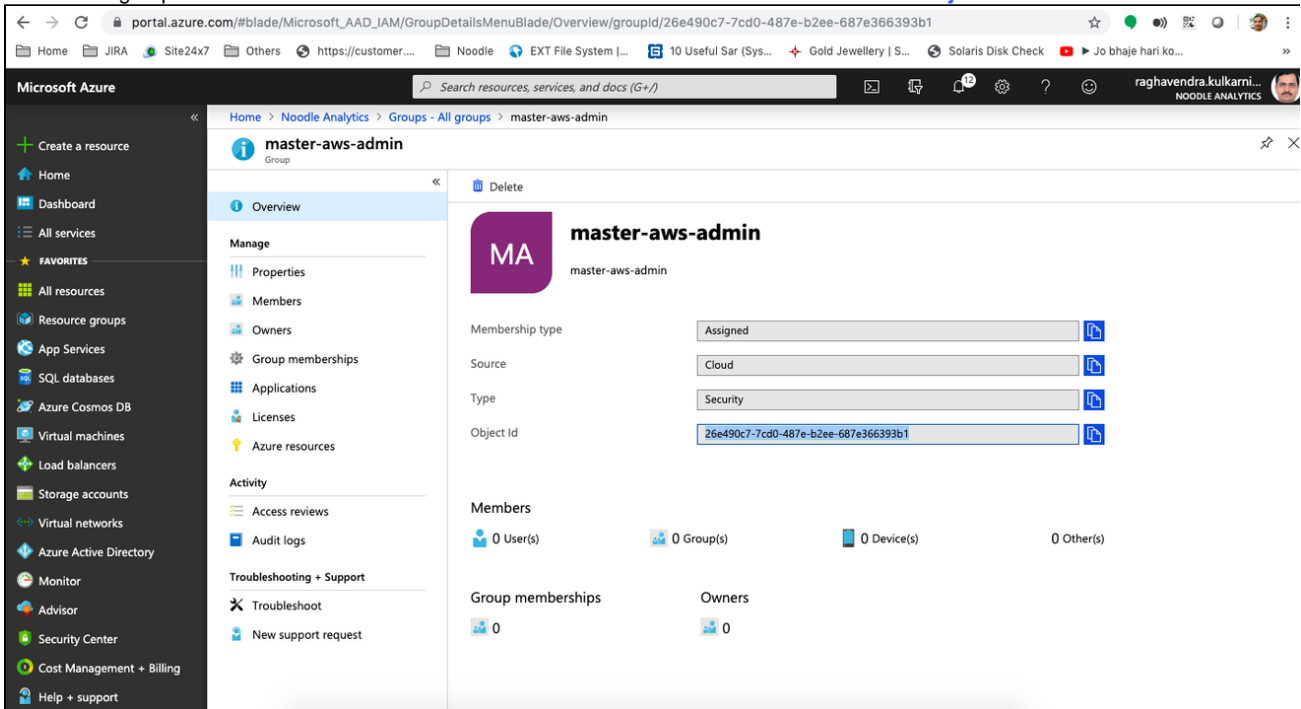
Please refer to the document before starting: <https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/aws-multi-accounts-tutorial>

This page will drive through adding more AWS accounts to this process.

- Download the metadata file from the Azure portal : Azure AD Connect >> Enterprise Applications >> Amazon Web Services (AWS) >> Single Sign-on >> Click Download next to Federation Metadata XML
- Log into the AWS account which needs this integration with local IAM user and MFA or root account in worst case
- Navigate to IAM service >> Identity providers
- Create Provider >> Provider Type >> SAML >> Name **WAAD** >> Metadata File >> Next Step >> Create
- Navigate to Roles >> Create Role >> SAML 2.0 federation >> SAML Provider **WAAD** >> Allow programmatic and AWS Management Console access >> Next: Permissions >> Search Administrator Access & Check Box >> Next: Tags >> Key: Name, Value: XXXX-aws-admin where XXXX is the account name all in lower case >> Next: Review >> Role Name: XXXX-aws-admin and Description also same >> Create Role
- Similarly create remaining other roles like XXXX-finance-admin, XXXX-read-only-user, XXXX-devops-user, XXXX-tpm-user with different policies to be attached. Later also these role policies can be changed as per requirements per AWS account but its always better to keep same policies for each role across the AWS accounts
- Once done, please make a note of account ID for that AWS account either from EC2 properties or IAM dashboard as highlighted below:



- Now login to Azure Portal and navigate to Groups: https://portal.azure.com/#blade/Microsoft_AAD_IAM/GroupsManagementMenuBlade/AllGroups
- Create new groups with the same name as that of IAM Roles created earlier and **note down the Object Ids of these** :



- Once all these groups are created and Object IDs are noted down, login to Microsoft Graph Explorer: URL
- Select GET >> beta >> <https://graph.microsoft.com/beta/servicePrincipals/750b8f24-1b2d-491f-8f12-34e1028513ac> >> Run Query
- Please note that the above link has Service Principal of the existing AWS Application from Azure AD, if the result fails then this ID might have changed
- **DONOT use DELETE option from the menu, this will remove entire AWS Enterprise application from your Azure Subscription with only the App registration entry left behind**
- Ideally in the Response Preview it shows the Manifest of the application with all the details:
- Now add the below section in the Request Body, making necessary changes to the content as per above details like AD group name, group ID, SAML provider ID

```
{
  "allowedMemberTypes": [
    "User"
  ],
  "description": "nw-devops-user,WAAD",
  "displayName": "nw-devops-user,WAAD",
  "id": "b361ae96-ccd7-471a-a7cc-88153788131f",
  "isEnabled": true,
  "origin": "ServicePrincipal",
  "value":
"arn:aws:iam::512088425928:role/nw-devops-user,arn:aws:iam::5120884
25928:saml-provider/WAAD"
}
```

- Duplicate this as many times based on number of AD groups created with , between the second to fourth flower bracket closure and leave the last one without , Example below is for XXXX account where only 2 roles and ad groups were created.

```
• {
  "allowedMemberTypes": [
    "User"
  ],
  "description": "master-aws-admin,WAAD",
  "displayName": "master-aws-admin,WAAD",
  "id": "26e490c7-7cd0-487e-b2ee-687e366393b1",
  "isEnabled": true,
  "origin": "ServicePrincipal",
  "value":
"arn:aws:iam::ACCOUNTID:role/master-aws-admin,arn:aws:iam::ACCOUNTI
D:saml-provider/WAAD"
}
```

Replace the name to the role/AD group names that were created for this AWS account, id to be replaced with the Object ID of the AD group that we created and also account number should also be updated as below:

```

{
  "allowedMemberTypes": [
    "User"
  ],
  "description": "master-aws-admin,WAAD",
  "displayName": "master-aws-admin,WAAD",
  "id": "26e490c7-7cd0-487e-b2ee-687e366393b1",
  "isEnabled": true,
  "origin": "ServicePrincipal",
  "value":
"arn:aws:iam::ACCOUNTID:role/master-aws-admin,arn:aws:iam::ACCOUNTID:saml-provider/WAAD"
  },
  {
    "allowedMemberTypes": [
      "User"
    ],
    "description": "master-finance-admin,WAAD",
    "displayName": "master-finance-admin,WAAD",
    "id": "8181dec7-1b39-4df3-9cc1-736af2cf5704",
    "isEnabled": true,
    "origin": "ServicePrincipal",
    "value":
"arn:aws:iam::ACCOUNTID:role/master-finance-admin,arn:aws:iam::ACCOUNTID:saml-provider/WAAD"
  }
}

```

- Double check id of the role/group to the Object id from Azure AD Group properties, account ID and names of the roles
- Once verified, copy this content in the Graph Explorer Request Body appending next to the section from where it was copied from. Make sure there is proper , and json validation done
- Now Select **Patch** >> beta >> same URL with Service principal >> Run Query
- Now Select **Get** >> beta >> same URL with Service principal >> Run Query and verify that the new entry has come in the response body, as below:

Microsoft | Microsoft Graph Solutions | Graph Explorer Getting Started | Docs API Reference Resources | Programs | All Microsoft | Search | Sign in

Graph Explorer

Authentication

Raghavendra Kulkarni
raghavendra.kulkarni@noodle.ai
modify permissions sign out

Sample Queries

Getting Started

- GET my profile
- GET my photo
- GET my mail
- GET all the items in my drive
- GET items trending around me
- GET my manager

show more samples

History

- GET /beta/servicePrincipals/750b8f24-1b2d-491f-8f12-34e1028513ac 200 2 minutes ago 387 ms
- PATCH /beta/servicePrincipals/750b8f24-1b2d-491f-8f12-34e1028513ac

Request Body

```
{
  "description": "master-aws-admin, WAAD",
  "displayName": "master-aws-admin, WAAD",
  "id": "26e490c7-7cd0-487e-b2ee-687e366393b1",
  "isEnabled": true,
  "origin": "ServicePrincipal",
  "value": "arn:aws:iam:693629377736:role/master-aws-admin,arn:aws:iam:693629377736:saml-provider/WAAD"
}
```

Request Headers

master-aws-admin

Success - Status Code 200, 387ms

Response Preview

```
{
  "allowedMemberTypes": [
    "User"
  ],
  "description": "master-aws-admin, WAAD",
  "displayName": "master-aws-admin, WAAD",
  "id": "26e490c7-7cd0-487e-b2ee-687e366393b1",
  "isEnabled": true,
  "origin": "ServicePrincipal",
  "value": "arn:aws:iam:693629377736:role/master-aws-admin,arn:aws:iam:693629377736:saml-provider/WAAD"
}
```

- Ideally this should return Success, it fails it will show error message which may be like miss placed comma or object id clash/duplicate or name duplicate, hence the previous step verification is very much important
- Once its Success here, navigate to AWS Application in Azure AD: https://portal.azure.com/#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/Users/objectId/750b8f24-1b2d-491f-8f12-34e1028513ac/appld/671e788b-fb2e-4bbb-a946-02305ced415f/menuitemId/QuickStart and go to Users and Groups
- Make sure that there is no entry of the Role Assigned that you are trying for the AWS account
- Click Add User >>Users and Groups >> Select and search for the group name >> under Role also select the same Name and click on Assign
- Repeat the same for other groups created for this account and make sure that group is assigned with same name Role ex. below:

Microsoft Azure

Search resources, services, and docs (G+)

Home > Amazon Web Services (AWS) - Users and groups

Amazon Web Services (AWS) - Users and groups

Enterprise Application

Overview

Getting started

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Users and groups

+ Add user Edit Remove Update Credentials Columns

The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

master

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
master-aws-admin	Group	master-aws-admin, WAAD
master-finance-admin	Group	master-finance-admin, WAAD

- Now to test, navigate to Single sign-on >> Test >> Sign in as current user as below:

portal.azure.com/#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/SignIn/objectId/750b8f24-1b2d-491f-8f12-34e1028513ac/appld/671e788b-fb2e-491f-8f12-34e1028513ac

Home JIRA Site24x7 Others https://customer... Noodle EXT File System 10 Useful Sys... Gold Jewellery | S... Solaris Disk Check Jo bhaje hari ko...

Microsoft Azure

Search resources, services, and docs (G+)

Home > Amazon Web Services (AWS) - Single sign-on >

Amazon Web Services (AWS) - SAML-bas

Enterprise Application

Overview

Getting started

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Users and groups
- Single sign-on
- Provisioning
- Self-service
- Security
- Conditional Access

Upload

Microsoft recommends installing the My Apps Secure Sign-in Extension for automatic error capture and resolution guidance.

Please make sure you have configured Amazon Web Services (AWS) before testing.

Sign in as current user

Sign in as someone else (requires browser extension)

Resolving errors

If you encounter an error in the sign-in page, please paste it below. If you still see the same issue, please wait for couple of minutes and retry.

What does the error look like?


```
{
  "Request Id": 4f8ec053-fb71-47de-a010-2786a32f1900
  "Correlation Id": 5aa879f5-68f1-482a-a405-f993d8f4cb0
  "Timestamp": 2018-03-06T23:54:10Z
  "Message": Error AADSTSXXXXX
}
```

Get resolution guidance

- This should now show the account that you have configured (highlighted below) with ONLY those groups which you are part of:

← → ↻ signin.aws.amazon.com/saml

Home JIRA Site24x7 Others <https://customer...> Noodle EXT File System [10 Useful Sar (Sys... Gold Jewell



Select a role:

▼ Account: noodleai (693629377736)

☐ master-aws-admin

▼ Account: noodleai-eaip (221191849743)

☐ eaip-aws-admin

☐ eaip-read-only-user

▼ Account: noodleway (512088425928)

☐ nw-aws-admin

☐ nw-read-only-user

[Sign In](#)

English

[Terms of Use](#) [Privacy Policy](#) © 1996-2019, Amazon Web Services, Inc. or its affiliates.

-
- Select the newly added AWS account and Role to login and confirm that all the configurations are successful